Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective

Year: 2021 | Citations: 214 | Authors: Iqbal H. Sarker

Abstract

Deep learning, which is originated from an artificial neural network (ANN), is one of the major technologies of today's smart cybersecurity systems or policies to function in an intelligent manner. Popular deep learning techniques, such as multi-layer perceptron, convolutional neural network, recurrent neural network or long short-term memory, self-organizing map, auto-encoder, restricted Boltzmann machine, deep belief networks, generative adversarial network, deep transfer learning, as well as deep reinforcement learning, or their ensembles and hybrid approaches can be used to intelligently tackle the diverse cybersecurity issues. In this paper, we aim to present a comprehensive overview from the perspective of these neural networks and deep learning techniques according to today's diverse needs. We also discuss the applicability of these techniques in various cybersecurity tasks such as intrusion detection, identification of malware or botnets, phishing, predicting cyberattacks, e.g. denial of service, fraud detection or cyberanomalies, etc. Finally, we highlight several research issues and future directions within the scope of our study in the field. Overall, the ultimate goal of this paper is to serve as a reference point and guidelines for the academia and professionals in the cyber industries, especially from the deep learning point of view.